
ASUS
Internet Security Router
ASUS

Asus Internet Security Router User Manual

1
2
Table Of Contents
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

Table of Contents

-

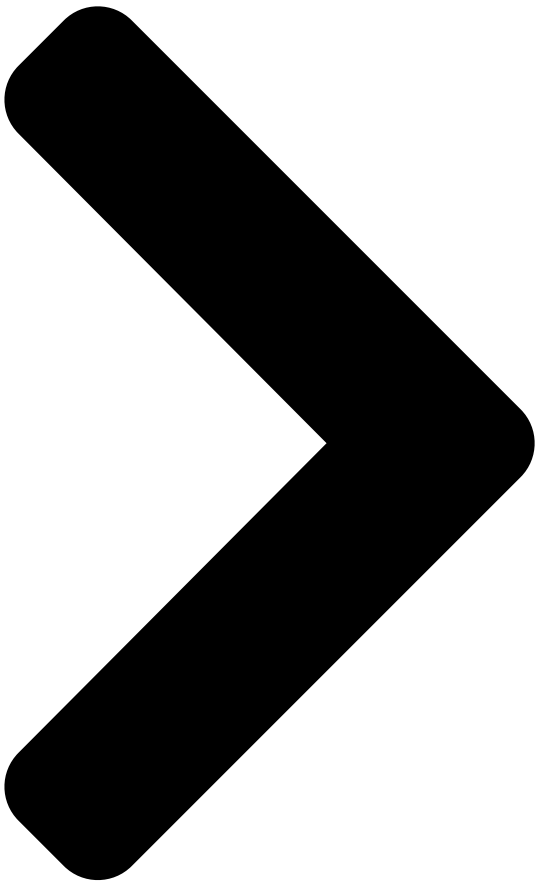
Troubleshooting

-

Bookmarks

Quick Links

Download this manual



Internet Security Router

User's Manual

Revision 1.1
Oct. 30, 2003

Table of Contents

Next Page

Related Manuals for Asus Internet Security Router

TV Converter Box ASUS TV Box User Manual

(23 pages)

Network Router Asus INET-810 User Manual

(90 pages)

Network Router Asus ISDNLINK INET-810 User Manual

(20 pages)

Network Router Asus ISDNLink INET-800 User Manual

(84 pages)

Network Router Asus RT-N66U Dark Knight User Manual

Dual-band wireless-n900 gigabit router (70 pages)

Network Router Asus ZenWiFi AX User Manual

Wireless ax6600 tri band router (151 pages)

Network Router Asus RT-AX55 User Manual

Dual band wi-fi router (103 pages)

Network Router Asus TUF-AX3000 V2 Quick Start Manual

Tuf gaming ax3000 v2 dual band wifi 6 router (2 pages)

Network Router Asus GX-D1051 Quick Start Manual

10/100/1000mbps gigabit ethernet switch (9 pages)

Network Router Asus RT-AC56U User Manual

Dual band wireless-ac1200 gigabit router (30 pages)

Network Router Asus RT-AX86U Quick Start Manual

Wireless-ax5700 dual-band gigabit router (36 pages)

Network Router Asus RT-AC66R User Manual

Dual band 3x3 802.11ac gigabit router (70 pages)

Network Router Asus DSL-AC68U User Manual

Dual-band 802.11ac wi-fi adsl/vdsl modem router (70 pages)

Network Router Asus RT-AC87R User Manual

Dual band 4x4 wireless ac2400 gigabit router (129 pages)

Network Router Asus RT-AX86U PRO User Manual

Wireless-ax5700 dual-band gigabit router (130 pages)

Network Router Asus RT-AC66U B1 User Manual

Wireless-ac 1750 dual band gigabit router (127 pages)

Summary of Contents for Asus Internet Security Router

Page 1: Internet Security

Internet Security Router User’s Manual Revision 1.1 Oct. 30, 2003...

Page 2

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

Page 3: Table Of Contents

Table of Contents Introduction.....1 Features .....1 System

Requirements..... 1 Using this Document .....1 1.3.1 Notational conventions .....1 1.3.2 Typographical conventions ..... 1 1.3.3 Special messages.....1 Getting to Know the Internet Security Router .....3 Parts List ..... 3 Front Panel.....

Page 4 3.1.4 Step 4. Turn on the Internet Security Router, the ADSL or cable modem and power up your computers.....10 Part 2 — Configuring Your Computers..... 11 3.2.1 Before you begin.....11 3.2.2 Windows® XP PCs:..... 11 3.2.3 Windows® 2000 PCs: .....11 3.2.4...

Page 5 5.3.2 Assigning DNS Addresses..... 29 5.3.3 Configuring DNS Relay .....29 Viewing LAN Statistics .....30 Configuring WAN Settings ..... 31 WAN Connection Mode .....31 PPPoE.....31 6.2.1 WAN PPPoE Configuration Parameters.....31 6.2.2 Configuring PPPoE for WAN .....32 Dynamic IP.....

Page 6 Configuring Firewall/NAT Settings..45 Firewall Overview .....45 9.1.1 Stateful Packet Inspection..... 45 9.1.2 DoS (Denial of Service) Protection.....45 9.1.3 Firewall and Access Control List (ACL)..... 45 9.1.3.1 Priority Order of ACL Rule.....45 9.1.3.2 Tracking Connection State .....46 9.1.4 Default ACL Rules .....

Page 7 9.5.5 Delete an URL Filter Rule ..... 59 9.5.6 View Configured URL Filter Rules.....59 9.5.7 URL Filter Rule Example.....59 Configuring Advanced Firewall Features – (Firewall è Advanced)....60 9.6.1 Configuring Self Access Rules .....60 9.6.1.1 Self Access Configuration Parameters.....61 Access Self Access Rule Configuration Page –...

Page 8 Access IP Pool Configuration Page – (Firewall è Policy List è 9.7.2.2 IP Pool) .....74 9.7.2.3 Add an IP Pool .....74 9.7.2.4 Modify an IP Pool .....74 9.7.2.5 Delete an IP Pool .....75 9.7.2.6 IP Pool Example.....75 9.7.3 Configuring NAT Pool.....

Page 9 VPN Connection Examples ..... 96 Intranet Scenario – firewall + VPN and no NAT for VPN traffic....96 10.6.1 10.6.1.1 Configure Rules on Internet Security Router 1 (ISR1) ....97 10.6.1.2 Configure Rules on Internet Security Router 2 (ISR2) ....98 10.6.1.3 Establish Tunnel and Verify.....

Page 10 12.5.2 Backup System Configuration .....127 12.5.3 Restore System Configuration.....127 12.6 Upgrade Firmware.....128 12.7 Reset the Internet Security Router.....129 12.8 Logout Configuration Manager.....130 ALG Configuration..... 131 IP Addresses, Network Masks, and Subnets .....135 14.1 IP Addresses ..... 135 14.1.1...

Page 11 Index ..... 149 List of Figures Figure 2.1. Front Panel LEDs..... 3 Figure 2.2. Rear Panel Connections..... 3 Figure 3.1. Overview of Hardware Connections ..... 10 Figure 3.2. Login Screen.....14 Figure 3.3. Setup Wizard Home Page.....15 Figure 3.4. Setup Wizard – Password Configuration Page.....15 Figure 3.5.

Page 12 Figure 9.4 NAPT – Map Any Internal PCs to a Single Global IP Address .....48 Figure 9.5 Reverse Static NAT – Map a Global IP Address to An Internal PC ..... 48 Figure 9.6 Reverse NAPT – Relayed Incoming Packets to the Internal Host Base on the Protocol, Port Number or IP Address .....

Page 13 Figure 10.4. Typical Intranet Network Diagram ..... 97 Figure 10.5. Intranet VPN Policy Configuration on ISR1.....98 Figure 10.6. Intranet VPN Policy Configuration on ISR2.....99 Figure 10.7. Typical Extranet Network Diagram .....101 Figure 10.8. Extranet Example –VPN Policy Configuration on ISR1 .....102 Figure 10.9.

Page 14 Table 2.1. Front Panel Label and LEDs .....3 Table 2.2. Rear Panel Labels and LEDs .....4 Table 2.3. DoS Attacks ..... 5 Table 2.4. VPN Features of the Internet Security Router.....7 Table 3.1. LED Indicators .....10 Table 3.2. Default Settings Summary.....20 Table 4.1.

Page 15 Table 9.10. Time Range Configuration Parameters .....80 Table 10.1. Default Connections in the Internet Security Router.....85 Table 10.2. Pre-configured IKE proposals in the Internet Security Router .....85 Table 10.3. Pre-configured IPSec proposals

in the Internet Security Router .....86 Table 10.4.

Page 17: Introduction

Internet using your high-speed broadband connection such as those with ADSL or cable modem. This User Manual will show you how to set up the Internet Security Router, and how to customize its configuration to get the most out of this product.

Page 18

Chapter 1. Introduction Internet Security Router User's Manual Provides clarification or non-essential information on the current topic. Note Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary. Definition Provides messages of high importance, including messages relating to personal safety or system integrity.

Page 19: Getting To Know The Internet Security Router

Chapter 2. Getting to Know the Internet Security Router Getting to Know the Internet Security Router Parts List In addition to this document, your Internet Security Router should come with the following: „ The Internet Security Router „ Power adapter „...

Page 20: Major Features

2.4.1 Firewall Features The Firewall as implemented in the Internet Security Router provides the following features to protect your network from being attacked and to prevent your network from being used as the springboard for attacks. „ Address Sharing and Management „...

Page 21: Acl (Access Control List)

"WinNuke", a widely used program to remotely crash unprotected Windows systems in the Internet. The Internet Security Router Firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, Reassembly and SYN flooding.

Page 22: Application Command Filtering

2.4.1.7 Log and Alerts Events in the network, that could be attempts to affect its security, are recorded in the Internet Security Router System log file. Event details are recorded in WELF (WebTrends Enhanced Log Format) format so that statistical tools can be used to generate custom reports.

Page 23: Remote Access

Security Router is intended to resolve these issues at an affordable price. The VPN supported by the Internet Security Router is IPSec compliant. Packets sent via VPN are encrypted to maintain privacy. The encrypted packets are then tunneled through a public network. As a result, tunnel participants enjoy the same security features and facilities that are available only to members of private networks at a reduced cost.

Page 24

Chapter 2. Getting to Know the Internet Security Router Internet Security Router User's Manual „ Remote Access VPN – Corporations use VPN to establish secure, end-to-end private network connections over a public networking infrastructure. VPN have become the logical solution for remote access connectivity.

Page 25: Quick Start Guide

Step 1. Connect an ADSL or a cable modem. For the Internet Security Router: Connect one end of the Ethernet cable to the port labeled WAN on the rear panel of the device. Connect the other end to the Ethernet port on the ADSL or cable modem.

Page 26: Step 4. Turn On The Internet Security Router, The Adsl Or Cable Modem And Power Up Your Computers

Press the Power switch on the rear panel of the Internet Security Router to the ON position. Turn on your ADSL or cable modem. Turn on and boot up your computer(s) and any LAN devices such as hubs or switches.

Page 27: Part 2 - Configuring Your Computers

Internet Security Router to do so. See "Assigning static IP Note addresses to your PCs" in page

13 for instructions. „ If you have connected your PC via Ethernet to the Internet Security Router, follow the instructions that correspond to the operating system installed on your PC. 3.2.2 Windows[CT6]®...

Page 28: Windows® 95, 98, And Me Pcs

10. In the TCP/IP Properties dialog box, click the “Default Gateway” tab. Enter 192.168.1.1 (the default LAN port IP address of the Internet Security Router) in the “New gateway” address field and click <Add> button to add the default gateway entry.

Page 29: Assigning Static Ip Addresses To Your Pcs

„ You maintain different subnets on your LAN. However, during the first time configuration of your Internet Security Router, you must assign an IP address in the 192.168.1.0 network for your PC, say 192.168.1.2, in order to establish connection between the Internet Security Router and your PC as the default LAN IP on Internet Security Router is pre-configured as 192.168.1.1.

Page 30: Part 3 - Quick Configuration Of The Internet Security Router

Internet connection. Your ISP should provide you with the necessary information to complete this step. Note the intent here is to quickly get the Internet Security Router up and running, instructions are concise. You may refer to corresponding chapters for more details.

Page 31: Figure 3.3. Setup Wizard Home Page

Internet Security Router User’s Manual Chapter 3. Quick Start Guide 3. Enter your user name and password, and then click to enter the Configuration Manager. The first time you log into this program, use these defaults: Default User Name: admin...

Page 32: Figure 3.5. Setup Wizard - System Identity Configuration Page

Figure 3.6. Setup Wizard – Date/Time Configuration Page 6. Set the time zone for the Internet Security Router by selecting your time zone from the Time Zone drop-down list. Click to save the settings and then click on the button to go to the next configuration page.

Page 33: Figure 3.7. Setup Wizard - Lan Ip Configuration Page

9. Now we are at the last page of the Setup Wizard, which is to configure the WAN settings for the Internet Security Router. Depending on the connection mode required for your ISP, you can select from the following three connection modes from the Connection Mode drop-down list (see...

Page 34: Figure 3.9. Setup Wizard - Wan Pppoe Configuration Page

Chapter 3. Quick Start Guide Internet Security Router User’s Manual Connection Mode drop-down list Figure 3.9. Setup Wizard – WAN PPPoE Configuration Page Connection Mode drop-down list Figure 3.10. Setup Wizard – WAN Dynamic IP Configuration Page a) PPPoE Connection Mode (see Figure 3.9) You don’t need to enter primary/secondary DNS IP addresses as PPPoE is able to...

Page 35: Figure 3.11. Setup Wizard - Wan Static Ip Configuration Page

Internet Security Router User’s Manual Chapter 3. Quick Start Guide Host name is optional. You may leave it empty if your ISP did not provide such information. Enter the user name and password provided by your ISP. Click on button to save the PPPoE settings.

Page 36: Testing Your Setup

3.3.3 Testing Your Setup At this point, the Internet Security Router should enable any computer on your LAN to use the Internet Security Router’s ADSL or cable modem connection to access the Internet. To test the Internet connection, open your web browser, and type the URL of any external website (such as http://www.asus.com).

Page 37: Getting Started With The Configuration Manager

The Configuration Manager program is preinstalled on the Internet Security Router. To access the program, you need the following: „ A computer connected to the LAN or WAN port on the Internet Security Router as described in the Quick Start Guide chapter.

Page 38: Functional Layout

Chapter 4. Getting Started with the Configuration Manager Internet Security Router User's Manual You can change the password at any time (see section 12.2 Change the Login Password on page 124). Note The Setup Wizard page displays each time you log into the program (shown in Figure 4.3 on page 23).

Page 39: The Home Page Of Configuration Manager

Internet Security Router User's Manual Chapter 4. Getting Started with the Configuration Manager Button/Icon Function Adds the existing configuration to the system, e.g. a static route or a firewall ACL rule and etc. Modifies the existing configuration in the system, e.g. a static route or a firewall ACL rule and etc.

Page 40: Figure 4.4. System Information Page

Chapter 4. Getting Started with the Configuration Manager Internet Security Router User's Manual Figure 4.4. System Information Page...

Page 41: Configuring Lan Settings

LAN IP Address If you are using the Internet Security Router with multiple PCs on your LAN, you must connect the LAN via the Ethernet ports on the built-in Ethernet switch. You must assign a unique IP address to each device residing on your LAN.

Page 42: Dhcp (Dynamic Host Control Protocol)

IP information to computers on a network. When you enable DHCP on a network, you allow a device — such as the Internet Security Router — to assign temporary IP addresses to your computers whenever they connect to your network. The assigning device is called a DHCP server, and the receiving device is a DHCP client.

Page 43: Why Use Dhcp

5.2.3 Configuring DHCP Server By default, the Internet Security Router is configured as a DHCP server on the LAN side, with a predefined IP address pool of 192.168.1.10 through 192.168.1.42 (subnet mask 255.255.255.0). To change this range of addresses, follow the Note procedures described in this section.

Page 44: Viewing Current Dhcp Address Assignments

Viewing Current DHCP Address Assignments When the Internet Security Router functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, just go to the DHCP Server Configuration page.

Page 45: Dns

In either case, you can specify the actual addresses of the ISP's DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN port on the Internet Security Router (e.g., 192.168.1.1). When you specify the LAN port IP address, the device performs DNS relay, as described in the following section.

Page 46: Viewing Lan Statistics

Viewing LAN Statistics You can view statistics of your LAN traffic on the Internet Security Router. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

Page 47: Configuring Wan Settings

Chapter 6. Configuring WAN Settings Configuring WAN Settings This chapter describes how to configure WAN settings for the WAN interface on the Internet Security Router that communicates with your ISP. You'll learn to configure IP address, DHCP and DNS server for your WAN in this chapter.

Page 48: Configuring Pppoe For Wan

Enable this option if you wish to keep your Internet connection active, even when there is no traffic. Enter the value for the "Echo Interval" at which you want the Internet Security Router to

send out some data periodically to your ISP. The default value of “Echo Interval” is 60 second.

Page 49: Configuring Dynamic Ip For Wan

Internet Security Router User’s Manual Chapter 6. Configuring WAN Settings Field Description Host Name Host name is optional but may be required by some ISP. Primary/ Secondary IP address of the primary and/or secondary DNS are optional as DHCP client will automatically obtain the DNS IP addresses configured at your ISP.

Page 50: Static Ip

Gateway Address Gateway IP address provided by your ISP. It must be in the same subnet as the WAN on the Internet Security Router. Primary/ Secondary You must at least enter the IP address of the primary DNS server. Secondary DNS is optional 6.4.2...

Page 51: Viewing Wan Statistics

Internet Security Router User’s Manual Chapter 6. Configuring WAN Settings 5. Enter the IP address of the primary DNS server. This information should be provided by your ISP. Secondary DNS server is optional. 6. Click to save the static IP settings when you are done with the configuration. You’ll see a summary of the WAN configuration at the bottom half of the configuration page.

Page 53: Configuring Routes

Quick Start Guide instructions, Part 2.) „ On the Internet Security Router itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection.

Page 54: Dynamic Routing Using Rip (Routing Information Protocol)

Chapter 7. Configuring Routes Internet Security Router User’s Manual Dynamic Routing using RIP (Routing Information Protocol) RIP enables routing information exchange between routers; thus, routes are updated automatically without human intervention. It is recommended that you enable RIP in the System Services Configuration Page as shown in Figure 12.1.

Page 55: Viewing The Static Routing Table

This table is known as the device’s routing table. To view the Internet Security Router’s routing table, click the Routing menu. The Static Routing Table displays at the bottom half of the Static Routing Configuration page, as shown in Figure 7.1: The Static Routing Table displays a row for each existing route containing the IP address of the destination network, subnet mask of destination network and the IP of the gateway that forwards the traffic.

Page 57: Configuring Ddns

Any interface status change to an external interface sends a DDNS update to the DNS server. When connection to Primary DNS server fails, the Internet Security Router updates the Secondary DNS server. When a DNS update is forced by the administrator, update is sent to the server for all active external interfaces.

Page 58: Ddns Configuration Parameters

Security Router has to be configured in the System Information Setup page properly. For example, If the host name of your Internet Security Router is “host1” and the DNS Zone Name is “yourdomain.com”, The fully qualify domain name (FQDN) is “host1.yourdomain.com”.)

Page 59: Access Ddns Configuration Page

Microsoft Knowledge Base article “Q317590: Configure DNS Dynamic Update in Windows 2000”, for details. 2. Make sure that you have a host name configured for the Internet Security Router; otherwise, go to the System Information Configuration page (System Management è System Identity) to configure one.

Page 60: Configuring Http Ddns Client

2. Make sure that you have a host name configured for the Internet Security Router; otherwise, go to the System Information Configuration page (System Management è System Identity) to configure one. 3. Open the DDNS Configuration page (see section 8.2 Access DDNS

Configuration Page).

Page 61: Configuring Firewall/Nat Settings

„ View firewall statistics. Note: When you define an ACL rule, you instruct the Internet Security Router to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the network or...

Page 62: Tracking Connection State

WARNING NAT Overview Network Address Translation allows use of a single device, such as the Internet Security Router, to act as an agent between the Internet (public network) and a local (private) network. This means that a NAT IP address can represent an entire group of computers to any entity outside a network.

Page 63: Dynamic Nat

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Figure 9.1 Static NAT – Mapping Four Private IP Addresses to Four Globally Valid IP Addresses 9.2.2 Dynamic NAT Dynamic NAT maps an internal host dynamically to a globally valid Internet address (m-to-n). The mapping usually contains a pool of internal IP addresses (m) and a pool of globally valid Internet IP addresses (n) with m usually greater than n.

Page 64: Napt (Network Address And Port Translation) Or Pat (Port Address Translation)

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual 9.2.3 NAPT (Network Address and Port Translation) or PAT (Port Address Translation) Also called IP Masquerading, this feature maps many internal hosts to one globally valid Internet address. The mapping contains a pool of network ports to be used for translation. Every packet is translated with the globally valid Internet address and the port number is translated with an un-used port from the pool of network ports.

Page 65: Reverse Static Nat

Reverse NAPT is also called inbound mapping, port mapping, or virtual server. Any packet coming to the Internet Security Router can be relayed to the internal host based on the protocol, port number and/or IP address specified in the ACL rule. This is useful when multiple services are hosted on different internal machines.

Page 66

Mave to This option allows you to set a priority for this rule. The Internet Security Router Firewall acts on packets based on the priority of the rules. Set a priority by specifying a number for its position in the...

Page 67

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Field Description IP Address, Subnet, Select any of these options and enter details as described in the Source IP Range and IP Pool section above. Source Port This option allows you to set the source port to which this rule should apply. Use the drop-down list to...

Page 68: Access Inbound Acl Rule Configuration Page - (Firewall È Inbound Acl)

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Field Description associate with an inbound ACL rule. Time Ranges Select a pre-configured time range during which the rule is active. Select "Always" to make the rule active at all times.

Page 69: Modify Inbound Acl Rules

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings 4. Make changes to any or all of the following fields: source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log, and VPN. Please see Table 9.1 for explanation of these fields.

Page 70: Outbound Acl Rule Configuration Parameters

Mave to This option allows you to set a priority for this rule. The Internet Security Router Firewall acts on packets based on the priority of the rules. Set a priority by specifying a number for its position in the...

Page 71 Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Field Description network. IP Address This option allows you to specify an IP address on which this rule will be applied. IP Address Specify the appropriate network address Subnet This option allows you to include all the computers that are connected in an IP subnet.

Page 72: Access Outbound Acl Rule Configuration Page - (Firewall È Outbound Acl)

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Field Description Single, Range Select any of these and enter details as described in the Source Port section above. Service This option allows you to select any of the pre-configured services (selectable from the drop-down list) instead of the destination port.

Page 73: Add An Outbound Acl Rule

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings 9.4.3 Add an Outbound ACL Rule To add an outbound ACL rule, follow the instructions below: 1. Open the Outbound ACL Rule Configuration Page (see section 9.4.2 Access Outbound ACL Rule Configuration Page).

Page 74: Delete Outbound Acl Rules

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual 4. Click on the button to modify this ACL rule. The new settings for this ACL rule will then be displayed in the outbound access control list table at the bottom half of the Outbound ACL Configuration page.

Page 75: Add An Url Filter Rule

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Figure 9.11. URL Filter Configuration Page 9.5.3 Add an URL Filter Rule To add an URL Filter, follow the instructions below: 1. Open the URL Configuration page (see section 9.5.2 Access URL Filter Configuration Page).

Page 76: Configuring Advanced Firewall Features - (Firewall È Advanced)

9.6.1 Configuring Self Access Rules Self Access rules control access to the Internet Security Router itself. You may use Self Access Rule Configuration page, as illustrated in Figure 9.13, to: „ Add a Self Access rule, and set basic parameters for it „...

Page 77: Self Access Configuration Parameters

Select the direction from which the traffic will be allowed. From LAN Select Enable or Disable to allow or deny traffic from the LAN (internal network) to the Internet Security Router. From WAN Select Enable or Disable to allow or deny traffic from WAN (external network) to the Internet Security Router.

Page 78: Modify A Self Access Rule

„ Add a new Self Access rule to: Allow TCP port 80 traffic (i.e. HTTP traffic) from the LAN and deny the HTTP traffic from the WAN port (i.e. from the external network) to the Internet Security Router. 9.6.1.4 Modify a Self Access Rule To modify a Self Access rule, follow the instructions below: 1.

Page 79: Service List Configuration Parameters

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Service drop-down list Edit icon Figure 9.14. Service List Configuration Page 9.6.2.1 Service List Configuration Parameters Table 9.5 describes the available configuration parameters for firewall service list. Table 9.5. Service List configuration parameters...

Page 80: Modify A Service

Windows systems in the Internet. The Internet Security Router Firewall also provides protection from a variety of common Internet attacks such as IP Spoofing, Ping of Death, Land Attack, Reassembly and SYN flooding. For a complete list of DoS protection provided by the Internet Security Router, please see Table 2.3.

Page 81 IP packet. This option is required if your connection to the ISP is through PPPoE. This data is used during transmission or reception of IP fragments. When large sized packets are sent via the Internet Security Router, the packets are chopped into fragments as large as MTU (Maximum Transmission Unit).

Page 82: Access Dos Configuration Page - (Firewall È Advanced È Dos)

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Field Description Minimum IP Enter the Minimum size of IP fragments to be allowed through Firewall. This Fragment Size limit will not be enforced on the last fragment of the packet. If the Internet traffic is such that it generates many small sized fragments, this value can be decreased.

Page 83: Configuring Application Filter

This high-performance content access control results in increased productivity, lower bandwidth usage and reduced legal liability. The Internet Security Router has the ability to handle active content filtering on certain application protocols such as HTTP, FTP, SMTP and RPC.

Page 84: Access Application Filter Configuration Page - (Firewall È Policy List È Application Filter)

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Field Description Allow or deny of change directory. LIST Allow or deny of Listing of files/directory. Allow or deny of Creating a directory. NLST Allow Short listing of directory contents.

Page 85: Add An Application Filter

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Figure 9.16. Application Filter Configuration Page 9.7.1.3 Add an Application Filter The application filter configuration is best explained with a few examples. Note that the configuration for RPC and SMTP is similar to that for FTP and will not be presented here.

Page 86: Figure 9.18. Ftp Filter Example - Configuring Ftp Filter Rule

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Filter Type drop-down list Filter Rule drop- down list Figure 9.18. FTP Filter Example – Configuring FTP Filter Rule 2. Select FTP from the Filter Type drop-down list. 3. Select "Add New Filter" from the Filter Rule drop-down list.

Page 87: Http Example: Add A Http Filter Rule To Block Java Applets And Java Archives

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings FTP filter drop-down list Figure 9.21. FTP Filter Example – Associate FTP Filter Rule to an ACL Rule 11. Associate the newly added FTP application filter rule to a firewall ACL rule (inbound, outbound or group ACL) by selecting a FTP filter from the FTP filter drop-down list (see Figure 9.21) and then...

Page 88: Modify An Application Filter

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual 7. Check the web application files to block – in this example, Java Applets and Java Archives 8. Enter additional web application files to block. Enter the file extension in the "Deny Following Files"...

Page 89: Delete An Application Filter

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Filter Type drop-down list Filter Rule drop- down list Figure 9.24. Modify an Application Filter 9.7.1.5 Delete an Application Filter To delete an Application Filter, click on the icon of the filter to be deleted or follow the instruction below: 1.

Page 90: Access Ip Pool Configuration Page - (Firewall È Policy List È Ip Pool)

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Field Description IP Address Enter the IP Address. Access IP Pool Configuration Page – (Firewall è Policy List è IP Pool) 9.7.2.2 Log into Configuration Manager as admin, click the Firewall menu, click the Policy List submenu and then click the IP Pool submenu.

Page 91: Delete An Ip Pool

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings 2. Click on the icon of the IP pool to be modified in the IP Pool List table or select the IP pool from the IP Pool drop-down list. 3. Make desired changes to any or all of the following fields: Pool name, Pool type and IP address.

Page 92: Configuring Nat Pool

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual Figure 9.27. IP Pool Example – Add Two IP Pools – MISgroup1 and MISgroup2 2. Associate an IP pool to firewall ACL rules – inbound, outbound or group ACL by selecting "IP Pool"...

Page 93: Access Nat Pool Configuration Page - (Firewall È Policy List È Nat Pool)

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Field Description Static Select this type of NAT to set a one-to-one Mapping between the Internal Address and the External Address. LAN IP range For the Internal Address Start IP Enter the starting IP address.

Page 94: Add A Nat Pool

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual 9.7.3.3 Add a NAT Pool To add a NAT Pool, follow the instructions below: 1. Open the NAT Pool Configuration page (see section 9.7.3.2 Access NAT Pool Configuration Page – (Firewall è Policy List è NAT Pool)).

Page 95: Figure 9.30. Network Diagram For Nat Pool Example

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings 10.64.2.0/24 Static NAT Pool WAN Port 10.64.2.1 10.64.2.254 10.64.2.2 10.64.2.3 LAN Port 192.168.1.1 192.168.1.11 192.168.1.12 192.168.1.13 Figure 9.30. Network Diagram for NAT Pool Example 1. Create a NAT pool for static NAT – see Figure 9.31.

Page 96: Configuring Time Range

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual NAT type drop-down list NAT pool drop-down list Figure 9.32. NAT Pool Example – Associate a NAT Pool to an ACL Rule 9.7.4 Configuring Time Range With this option you can configure access time range records for eventual association with ACL rules. ACL rules associated with a time range record will be active only during the scheduled period.

Page 97: Access Time Range Configuration Page - (Firewall È Policy List È Time Range)

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Access Time Range Configuration Page – (Firewall è Policy List è Time Range) 9.7.4.2 Log into Configuration Manager as admin, click the Firewall menu, click the Policy List submenu and then click the Time Range submenu.

Page 98: Delete A Time Range

Chapter 9. Configuring Firewall/NAT Settings Internet Security Router User's Manual 5. Click on the button to save the new settings. 9.7.4.5 Delete a Time Range To delete a Time Range, click on the icon of the Time Range to be deleted.

Page 99: Firewall Statistics - Firewall È Statistics

Internet Security Router User's Manual Chapter 9. Configuring Firewall/NAT Settings Firewall Statistics – Firewall è Statistics The Firewall Statistics page displays details regarding the active connections. Figure 9.36 shows a sample firewall statistics for active connections. To see an updated statistics, click on button.

Page 101: Configuring Vpn

The chapter contains instructions for configuring VPN connections using automatic keying and manual keys. 10.1 Default Parameters The Internet Security Router is pre-configured with a default set of proposals/connections. They cover the most commonly used sets of parameters, required for typical deployment scenarios. It is recommended that you use these pre-configured

proposals/connections to simplify VPN connection setup.

Page 102: Table 10.3. Pre-Configured Ipsec Proposals In The Internet Security Router

IPSec proposals decide the type of encryption and authentication for the traffic that flows between the endpoints of the tunnel. Table 10.3 lists the default IPSec proposals available on the Internet Security Router Table 10.3. Pre-configured IPSec proposals in the Internet Security Router...

Page 103: Vpn Tunnel Configuration Parameters

Move to This option allows you to set a priority for this rule. The VPN service in the Internet Security Router acts on packets based on the priority of the rule, with 1 being the highest priority. Set a priority by...

Page 104 Chapter 10. Configuring VPN Internet Security Router User's Manual Options Description VPN Connection Type Site to site Click this radio button to add a policy for site-to-site users. Remote access Click this radio button to add a policy for remote access users.

Page 105 Internet Security Router User's Manual Chapter 10. Configuring VPN Options Description Xauth (aggressive Xauth is a user ID and password based authentication. This option is mode only) available only when aggressive mode is selected. Preshared Key Enter the shared secret (this should match the secret key at the other end).

Page 106: Establish Vpn Connection Using Automatic Keying

Chapter 10. Configuring VPN Internet Security Router User's Manual Options Description Pre-shared Key Specific Options PFS Group PFS stands for perfect forward secrecy.You may choose to use the same keys (generated when the IKE tunnel is created) for all re-negotiations or you can choose to generate new keys for every re-negotiation.

Page 107: Add A Rule For Vpn Connection Using Pre-Shared Key

Internet Security Router User's Manual Chapter 10. Configuring VPN 10.3.1 Add a Rule for VPN Connection Using Pre-shared Key VPN Tunnel Configuration Page, as illustrated in the Figure 10.1, is used to configure a rule for VPN connection using pre-shared key...

Page 108: Modify Vpn Rules

Chapter 10. Configuring VPN Internet Security Router User's Manual 7. Assign a priority for this rule by selecting a number from the "Move to" drop-down list. Note that the number indicates the priority of the rule with two being the highest as one is used by the rule, allow-ike-io, which is needed by IKE.

Page 109: Establish Vpn Connection Using Manual Keys

Internet Security Router User's Manual Chapter 10. Configuring VPN 10.4 Establish VPN Connection Using Manual Keys This section describes the steps to establish the VPN tunnel-using manual keying. Manual keying is a method to achieve security when ease of configuration and maintenance is more important or automatic keying is not feasible due to interoperability issues between IKE implementations on the gateways.

Page 110: Modify Vpn Rules

Chapter 10. Configuring VPN Internet Security Router User's Manual 5. Click on "Enable" or "Disable" radio button to enable or disable this rule. 6. Make changes to any or all of the following fields: local/remote secure group, remote gateway, key management type (select Manual Key), pre-shared key for IKE, encryption/authentication algorithm for IKE, lifetime for IKE, encryption/authentication algorithm for IPSec, operation mode for IPSec, PFS group for IPSec and lifetime for IPSec.

Page 111: Vpn Statistics

Internet Security Router User's Manual Chapter 10. Configuring VPN Tunnel 1. Log into Configuration Manager as admin, click the VPN menu, and then click the VPN submenu. 2. The VPN rule table located at the bottom half of the VPN Configuration page shows all the configured VPN rules.

Page 112: Vpn Connection Examples

Security Router for the Intranet scenario using the following steps: „ Configure VPN connection rules. „ Configure Firewall access rules to allow inbound and outbound VPN traffic. „ Configure a Firewall self rule to allow IKE packets into the Internet Security Router.

Page 113: Configure Rules On Internet Security Router 1 (Isr1)

Internet Security Router User's Manual Chapter 10. Configuring VPN 10.6.1.1 Configure Rules on Internet Security Router 1 (ISR1) This section describes the steps to establish the VPN/Firewall for the Internet scenario. Figure 10.4 depicts the typical Intranet connections. Note that ADSL or cable modem is not required if the two networks are connected via Ethernet connections.The setting of each configuration step is illustrated in a figure.

Page 114: Configure Rules On Internet Security Router 2 (Isr2)

Table 10.7. Inbound Un-translated Firewall Rule for VPN Packets on ISR1 Field Value Type Subnet Source IP Address 192.168.2.0 Mask 255.255.255.0 Type Subnet Destination IP Address 192.168.1.0 Mask 255.255.255.0 None Action Allow Enable 10.6.1.2 Configure Rules on Internet Security Router 2 (ISR2) Step 1: Configure VPN connection rules...

Page 115: Figure 10.6. Intranet Vpn Policy Configuration On Isr2

Internet Security Router User's Manual Chapter 10. Configuring VPN Refer to the section 10.3 Establish VPN Connection Using Automatic Keying to configure VPN policies on ISR2 using automatic keying. Figure 10.6. Intranet VPN Policy Configuration on ISR2 Step 2: Configure Firewall rules 1.

Page 116: Establish Tunnel And Verify

Chapter 10. Configuring VPN Internet Security Router User's Manual Field Value Mask 255.255.255.0 None Action Allow Enable Note: The outbound Un-translated Firewall rule has to be added the existing rule ID 1001. Table 10.9. Inbound Un-translated Firewall Rule for VPN Packets on ISR1...

Page 117: Setup The Internet Security Routers

„ Configure VPN Connection rules. „ Configure Firewall rules to allow inbound and outbound VPN traffic by performing one-to-one NAT. „ Configure a Firewall Self Access rule to allow IKE packets into the Internet Security Router. 10.6.2.1 Setup the Internet Security Routers On ISR1 1.

Page 118: Configure Vpn Rules On Isr1

Chapter 10. Configuring VPN Internet Security Router User's Manual 5. Save the configuration. 10.6.2.2 Configure VPN Rules on ISR1 Step 1: Configure VPN Rule Refer to the section 10.3 Establish VPN Connection Using Automatic Keying to configure VPN policies on ISR1 using automatic keying with the following addresses: 1.

Page 119: Figure 10.9. Extranet Example - Outgoing Nat Pool Configuration On Isr1

Internet Security Router User's Manual Chapter 10. Configuring VPN Figure 10.9. Extranet Example – Outgoing NAT Pool Configuration on ISR1 2. Configure incoming static NAT pool (reverse-static-NAT) for translating addresses in range 192.168.11.1-192.168.11.254 to 192.168.1.1-192.168.1.254 Figure 10.10. Extranet Example – Incoming NAT Pool Configuration on ISR1 Step 3: Configure Extranet access rules 1.

Page 120: Configure Vpn Rules On Isr2

Chapter 10. Configuring VPN Internet Security Router User's Manual Figure 10.11. Extranet Example – Outbound ACL Rule on ISR1 2. Configure inbound Firewall rules to map the destination IP address of inbound packets from 192.168.11.x range to 192.168.1.x (defined by Incoming_NAT pool) range after the packet is processed by VPN.

Page 121: Figure 10.13. Extranet Example -Vpn Policy Configuration On Isr2

Internet Security Router User's Manual Chapter 10. Configuring VPN Refer to the section 10.3 Establish VPN Connection Using Automatic Keying to configure VPN policies on ISR2 using automatic keying with the following addresses: 1. Use 192.168.12.0/255.255.255.0 as Local

Secure Group 2.

Page 122: Figure 10.15. Extranet Example - Incoming Nat Pool Configuration On Isr2

Chapter 10. Configuring VPN Internet Security Router User's Manual 2. Configure incoming static NAT pool (reverse-static-NAT) for translating addresses in range 192.168.12.1-192.168.12.254 to 192.168.1.1-192.168.1.254 Figure 10.15. Extranet Example – Incoming NAT Pool Configuration on ISR2 Step 3: Configure Extranet rules 1.

Page 123: Establish Tunnel And Verify

Internet Security Router User's Manual Chapter 10. Configuring VPN Figure 10.17. Extranet Example – Inbound ACL Rule on ISR2 10.6.2.4 Establish Tunnel and Verify „ Start continuous ping from a host on the LAN behind ISR1 to a host on the LAN behind ISR2. The first few pings would fail.

Page 125: Configuring Remote Access

The Internet Security Router maintains details about the access policies defined for the remote access groups. These access lists define the resources the remote users are allowed to access and the inactivity time-out applicable to all the users in the group.

Page 126: Access User Group Configuration Page - (Remote Access È User Group)

Chapter 11. Configuring Remote Access Internet Security Router User's Manual Field Description User Name Enter a unique User name for the user that you would like to add. User State Click on the Enable or Disable radio button to enable or disable the user.

Page 127: Modify A User Group Or A User

Internet Security Router User's Manual Chapter 11. Configuring Remote Access 6. If you want to add a user to this newly created group, continue with the following steps; otherwise, jump to step 12 to complete the configuration. 7. Select "Add New User" from the user drop-down list.

Page 128: User Group And Users Configuration Example

Chapter 11. Configuring Remote Access Internet Security Router User's Manual 3. Click on the button to delete this user group. Note that a user group cannot be deleted unless all the users belong to the group are deleted first. To delete a user, simply click on the...

Page 129: Access Group Acl Configuration Page - (Remote Access È Group Acl)

For a user belonging to a user group to connect to the Internet Access Router, he or she must do a special login first to activate user group based policies; otherwise, the Internet Security Router will drop all the connection requests from the user. Users in a user group can enter the following URL in the browser in order to login to the Internet Security Router and activate associated access policies.

Page 130: Figure 11.4. Login Console

Chapter 11. Configuring Remote Access Internet Security Router User's Manual Figure 11.4. Login Console After a successful login, the screen appears as in Figure 11.5. Figure 11.5. Login Status Screen User Name: Richard Group Name: RoadWarrior User Name: Gloria Internet...

Page 131: Configure Firewall For Remote Access

Remote Access is usually used to support mobile users of a company to access their corporate network without compromising on security. The steps required for configuring the Internet Security Router for remote access is best explained with an example. The following shows the steps required to configure the Internet Security Router for the remote users, Richard and Gloria, to access the FTP server located in the protected network, i.e.

Page 132: Virtual Ip Address Configuration For Remote Access Vpn

To create an illusion of seamless integration (for the VPN remote access users) with your private network, the Internet Security Router allows you to assign a virtual IP address for each remote VPN user. Those remote VPN users can use VPN client software such as SafeNet SoftRemote or

SSH Sentinel VPN Client software to establish VPN connection between the Internet Security Router and the VPN client software.

Page 133: Change Virtual Ip Assignments For Remote Access Users

Internet Security Router User's Manual Chapter 11. Configuring Remote Access 5. An IP address (in the IP Address field) is automatically assigned for the selected user. However, you may change it to any desired value. 6. Click to save the virtual IP settings. Note that a list of existing virtual IP assignments is displayed at the bottom half of the VPN Virtual IP Configuration page.

Page 134: Configure Vpn For Remote Access

Remote Access VPN is used primarily by telecommuters/road-warriors to securely access resources behind the Internet Security Router located at a head-office or a central site. The steps required for configuring the Internet Security Router and the VPN client on a remote user's machine to provide remote access are explained in the following sections.

Page 135: Figure 11.12. Main Mode Remote Access Example - Configure The Virtual Ip Address

Internet Security Router User's Manual Chapter 11. Configuring Remote Access Figure 11.12. Main Mode Remote Access Example – Configure the Virtual IP address 3. Create a VPN policy for Richard and Gloria. The settings for this policy are illustrated in Figure 11.13.

Page 136: Aggressive Mode Remote Access

Security Router. Once these policies are instantiated, the remote user is allowed secure access through the Internet Security Router. Again, the example, see Figure 11.10, used to illustrate the main mode remote access is used here. Follow the instructions below to configure for aggressive mode remote access.

Page 137: Figure 11.16. Aggressive Mode Remote Access Example - Remote Vpn Connection Setup For "Roadwarrior" Group

Internet Security Router User's Manual Chapter 11. Configuring Remote Access 3. Create a VPN policy for Richard and Gloria. The settings for this policy are illustrated in Figure 11.16. Note that only one policy is needed for both Richard and Gloria because they belong to the same group, RoadWarrior.

Page 139: System Management

As shown in Figure 12.1, you can use the System Services Configuration page to enable or disable services supported by the Internet Security Router. All services, firewall, VPN, DNS, DHCP and RIP, are all enabled at the factory. To disable or enable individual service, follow the steps below: 1.

Page 140: Change The Login Password

Chapter 12. System Management Internet Security Router User's Manual 12.2 Change the Login Password The first time you log into the Configuration Manager, you use the default username and password (admin and admin). The system allows two types of users – administrator (username: admin) and guest (username: guest).

Page 141: Setup Date And Time

Figure 12.3. System Information Configuration Page 12.4 Setup Date and Time The Internet Security Router keeps a record of the current date and time, which it uses to calculate and report various performance data. Changing the Internet Security Router date and time does not affect the date and time on your PCs.

Page 142: View The System Date And Time

Figure 12.5. Default Setting Configuration Page Sometimes, you may find that you have no way to access the Internet Security Router, e.g. you forget your password. The only way out in this scenario is to reset the system configuration to the factory default by following the procedures below using the reset switch: 1.

Page 143: Backup System Configuration

Internet Security Router User's Manual Chapter 12. System Management 12.5.2 Backup System

Configuration Follow the steps below to backup system configuration: 1. Log into Configuration Manager as admin, click the System Management menu, click the Configuration submenu and then click the Backup submenu. The Backup Configuration page displays, as shown in Figure 12.6.

Page 144: Upgrade Firmware

Chapter 12. System Management Internet Security Router User's Manual Figure 12.7. Restore System Configuration Page 2. Enter the path and name of the system configuration file that you want to restore in the "Configuration File" text box. Alternatively, you may click on the button to search for the system configuration file on your hard drive.

Page 145: Reset The Internet Security Router

Note that after the transfer of firmware is completed, the Internet Security Router will reboot to make the new firmware in effect. 12.7 Reset the Internet Security Router To reset the Internet Security Router, click on the button in the Configuration Manager Reset page. Figure 12.10. Configuration Manager Reset Page...

Page 146: Logout Configuration Manager

Chapter 12. System Management Internet Security Router User's Manual 12.8 Logout Configuration Manager To logout of Configuration Manager, click on the button in the Configuration Manager Logout page. If you are using IE as your browser, a window similar to the one shown in Figure 12.12 will prompt for confirmation before closing your browser.

Page 147: Alg Configuration

Internet Security Router User's Manual Chapter 13. ALG Configuration ALG Configuration Table 13.1 lists all the supported ALGs (Application Layer Gateway). Table 13.1. Supported ALG ALG/Application Protocol and Port Predefined Service Tested Software Name Name Version PCAnywhere UDP/22 PC-ANYWHERE pcAnywhere 9.0.0...

Page 148

Chapter 13. ALG Configuration Internet Security Router User's Manual ALG/Application Protocol and Port Predefined Service Tested Software Name Name Version L2TP UDP/1701 L2TP Windows 2000 Server built-in UDP/53 PPTP TCP/1723 PPTP Windows 2000 Server built-in UDP/53 IPSec (Only Tunnel UDP/500...

Page 149

Internet Security Router User's Manual Chapter 13. ALG Configuration ALG/Application Protocol and Port Predefined Service Tested Software Name Name Version TCP/443 HTTPS TCP/80 HTTP UDP/53 Diablo II (BATTLE- TCP/4000 DIABLO-II Diablo II NET-TCP, BATTLE- TCP/ 6112 BATTLE-NET-TCP, NET-UDP) BATTLE-NET-UDP UDP/53...

Page 151: Ip Addresses, Network Masks, And Subnets

Internet Security Router User's Manual Chapter 14. IP Addresses, Network Masks, and Subnets IP Addresses, Network Masks, and Subnets 14.1 IP Addresses This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

Page 152: Subnet Masks

Chapter 14. IP Addresses, Network Masks, and Subnets Internet Security Router User's Manual Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Page 153

Internet Security Router User's Manual Chapter 14. IP Addresses, Network Masks, and Subnets Class C: 255.255.255.0 These are called default because they are used when a network is initially configured, at which time it has no subnets.

Page 155: Troubleshooting

LINK LAN LED does Verify that the Ethernet cable is securely connected to your LAN not illuminate after hub or PC and to the Internet Security Router. Make sure the Ethernet cable is PC and/or hub is turned on. attached.

Page 156: Diagnosing Problem Using Ip Utilities

Appendix 15. Troubleshooting Internet Security Router User's Manual Problem Troubleshooting Suggestion addresses within a predefined pool PCs cannot display Verify that the DNS server specified on the PCs is correct for web pages on the your ISP, as discussed in the item above. You can use the ping Internet.

Page 157: Nslookup

If the target computer cannot be located, you will receive the message "Request timed out." Using the ping command, you can test whether the path to the Internet Security Router is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

Page 158: Figure 15.2. Using The Nslookup Utility

Appendix 15. Troubleshooting Internet Security Router User's Manual Figure 15.2. Using the nslookup Utility There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

Page 159: Glossary

A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the Internet Security Router's interfaces can be configured as a DHCP relay. See DHCP. DHCP server...

Page 160 Appendix 16. Glossary Internet Security Router User's Manual element of URLs, which identify a specific file at a web site, e.g., http://www.asus.com. See also DNS. download To transfer data in the downstream direction, i.e., from the Internet to the user.

Page 161 Internet Security Router User's Manual Appendix 16. Glossary from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID.

Page 162 Appendix 16. Glossary Internet Security Router User's Manual between your ISP and your computer. The WAN interface on the Internet Security Router uses two forms of PPP called PPPoA and PPPoE. See also PPPoA, PPPoE. PPPoE Point-to-Point Protocol over Ethernet One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA.

Page 163 Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the Internet Security Router, WAN refers to the Internet. Web browser A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user.

Page 165: Index

Internet Security Router User's Manual Appendix 16. Glossary Index 100BASE-T, 143 defined, 29 10BASE-T, 143 relay, 29 ADSL, 143 Domain name, 143 authenticate, 143 Domain Name System. See DNS Binary numbers, 143 download, 144 Bits, 143 Broadband, 143 defined, 144...

Page 166 Appendix 17. Index Internet Security Router User's Manual Inbound ACL Configuration page, 49 MAC addresses, 145 Internet, 144 in DHCP Address Table, 28 troubleshooting access to, 139 Mask. See Network mask Intranet, 144 Mbps, 145 IP address in device's routing table, 39...

Page 167 Internet Security Router User's Manual Appendix 17. Index Routing Configuration, 37 Static routes Setup Wizard, 15, 23 adding, 38 User Password Configuration, 124 Statically assigned IP addresses, 27 WAN Statistics, 35 Subnet, 146 Pages Inbound ACL Configuration, 49 Subnet mask. See Network mask...

This manual is also suitable for:

SI1000Tv box